

**REMARKS**

This Preliminary Amendment is in response to the Advisory Action mailed February 27, 2006. Claims 12-14 have been cancelled without prejudice. Applicant respectfully traverses the §103(a) rejections and respectfully requests the Examiner to withdraw these rejections.

***Rejection Under 35 U.S.C. § 103***

Claims 1-14 and 22-23 were rejected under 35 U.S.C. §103(a) as being unpatentable over Rallis (U.S. Patent No. 6,425,084) in view of Adams (U.S. Patent No. 6,363,485). Moreover, claims 15-21 were rejected under 35 U.S.C. §103(a) as being unpatentable over Rallis in view of Adams and Lohstroh (U.S. Patent No. 5,953,419). Applicant respectfully traverses these rejections in their entirety because a *prima facie* case of obviousness has not been established.

As the Examiner is aware, to establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify a reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all of the claim limitations. *See MPEP §2143; see also In Re Fine, 873 F. 2d 1071, 5 U.S.P.Q.2d 1596 (Fed. Cir. 1988).* Herein, at a minimum, the combined teachings of the cited references do not describe or suggest all the claim limitations set forth in the above-noted claims.

**A. §103(A) REJECTION OF CLAIMS 1-14 AND 22-23**

Claims 1-14 and 22-23 were rejected under 35 U.S.C. §103(a) as being unpatentable over Rallis (U.S. Patent No. 6,425,084) in view of Adams (U.S. Patent No. 6,363,485). Applicant respectfully submits that a *prima facie* case of obviousness has not been established because neither Rallis nor Adams, alone or in combination, suggests every limitation set forth in the above-identified claims.

For instance, with respect to independent claim 1, the Advisory Action states that Rallis teaches an “user-validation program [that] ‘prompts the user to attach the key

device 20 to the notebook computer’, which indicates hat the keying material or the serial number is released in response to authenticating the user.” *See Page 2 of the Advisory Action.* Applicant respectfully disagrees with these findings because Rallis teaches the boot-up user-validation program where a key device serial number, considered by the Examiner to constitute the “first keying material” as claimed, is released *prior to* user authentication. This key device serial number is *not* released *after authenticating the user* as claimed. *Emphasis added.* Adams also fails to suggest this limitation as well.

Moreover, the Advisory Action states that Adams “teaches combining keying materials to produce a combination key.” Namely, the first and second keying material read on the first and second partial seeds and the combination key reads on the “secret encryption key”. *See Page 2 of the Advisory Action.* However, Applicant respectfully submits that such combination occurs during the boot process as claimed.

In addition, the Office Action states that Rallis teaches an operation to “decrypt a second BIOS area to recover a second segment of BIOS code.” *See Page 3 of the Office Action.* Applicant respectfully disagrees and respectfully submits that this ground for traverse has not been fully addressed by the Examiner. First, the limitation has been improperly parsed because claim 1 states “*using the combination key* to decrypt a second BIOS area to recover a second segment of BIOS code.” *Emphasis added.* There is no teaching by the combination of Rallis and Adams in using a combination key, the first keying material combined with a second keying material internally stored within the platform, to decrypt a second BIOS area to recover a second segment of BIOS code as claimed.

Secondly, the Advisory Action states that Adams now teaches the decryption of encrypted data by the secret key (see column 2, lines 58-62 of Adams). However, on column 5, lines 46-48, it appears that the “encrypted data” is directed to a user account file or other data that is clearly not a second area of BIOS code as claimed. Neither Rallis nor Adams, alone or in combination, suggest using a combination key being the first keying material (key device serial number) combined with a second keying material

internally stored within the platform in order to decrypt the second BIOS area (encrypted data) to recover a second segment of BIOS code. The separate authentication device appears to have no capability of accessing BIOS code internally stored within the platform (personal computer 212).

Hence, since neither Rallis nor Adams describe or suggest all of the claim limitations set forth in independent claim 1, a *prima facie* case of obviousness has not been established, and thus, the §103(a) rejection should be withdrawn.

Based on the dependency of claims 2-11 on independent claim 1, believed by Applicant to be in condition for allowance, no further discussion as to the grounds for traverse is warranted. Of course, it is evident that a *prima facie* case of obviousness cannot be established for many of the dependent claims, with respect for claim 3 as an example, because the validation records of Rallis are stored in a reserved sector of the hard disk (42), not BIOS ROM (30). *See col. 3, lines 62-64 of Rallis.* Also, Adams does not describe such BIOS storage as well. Hence, withdrawal of the §103(a) rejection as applied to claims 1-11 is respectfully requested.

#### B. §103(A) REJECTION OF CLAIMS 15-21

Moreover, Claims 15-21 were rejected under 35 U.S.C. §103(a) as being unpatentable over Rallis in view of Adams and Lohstroh (U.S. Patent No. 5,953,419). Applicant respectfully submits that a *prima facie* case of obviousness has not been established because neither Rallis, Adams nor Lohstroh, alone or in any combination, suggest every limitation set forth in the above-identified claims.

With respect to independent claims 15 and 19, Applicant incorporates the arguments set forth above in which the trusted platform module produces a combination key by combining a first incoming keying material *released after authentication of a user of the platform* with a second keying material. *Emphasis added.* In contrast and teaching away from the claimed invention, the teachings of Rallis are directed to the release of the first keying material (key device serial number) *as part of the user authentication procedure*, not the release of the first keying material after *authentication of a user of the platform* as claimed. *Emphasis added.*

In conclusion, the new combination of the teachings of Lohstroh in order to modify the teachings of Rallis (and Adams), namely modifying when first incoming keying material is released, is impermissible. The Federal Circuit has consistently held that the combination of references in support of a §103 rejection is improper when such combination is directed to the modification of an invention disclosed and it destroys the intent, purpose or function of the invention disclosed. *See In re Gordon*, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984). MPEP §2143.01. With respect to Rallis, the release of the key device serial number must occur during the authentication procedure, not after the procedure.

Hence, withdraw of the outstanding §103(a) rejection as applied to independent claims 15 and 19 as well as claims 16-18 and 20-21 dependent thereon is respectfully requested.

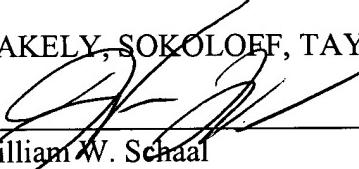
***Conclusion***

Applicant respectfully requests that a timely Notice of Allowance be issued in this case.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: March 6, 2006

By   
William W. Schaal  
Reg. No. 39,018  
Tel.: (714) 557-3800 (Pacific Coast)

12400 Wilshire Boulevard, Seventh Floor  
Los Angeles, California 90025

---

**CERTIFICATE OF MAILING/TRANSMISSION (37 CFR 1.8A)**

I hereby certify that this correspondence is, on the date shown below, being:

MAILING

FACSIMILE

deposited with the United States Postal Service  
as first class mail in an envelope addressed to:  
Commissioner for Patents, PO Box 1450,  
Alexandria, VA 22313-1450.

transmitted by facsimile to the Patent and  
Trademark Office.

Date: 2/6/2006

2/6/2006

  
Susan McFarlane

Date